



DISCOVERING PC-CONNECTED DEVICES

in HP Web Jetadmin

CONTENTS

Overview	2
Proxy agents vs. WMI	2
Comparison matrix	2
Proxy agents	3
Installation	3
Silent mode installation—HP SNMP Proxy Agent	3
Silent mode installation—HP WS Pro Proxy Agent	4
HP SNMP Proxy Agent	5
HP WS Pro Proxy Agent	5
Discovery	6
Device management	7
View device information	9
Set device configurations	9
Alerts	10
Reports	10
Proxy comparison	10
Supported devices	11
WMI	11
HP SNMP Proxy Agent	12
HP WS Pro Proxy Agent	12
Troubleshooting discovery	13
HP SNMP Proxy Agent	13
HP WS Pro Proxy Agent	16
Discovery logs	17
PC-connected discovery logging in HP Web Jetadmin	17
HP SNMP Proxy Agent logging	18
HP WS Pro Proxy logging	23
WMI	23
Performance	25
Summary	25
Appendix A—Supported printing devices	26
HP SNMP Proxy Agent, supported legacy devices	26
HP SNMP Proxy Agent, not supported: HP FutureSmart devices	27
HP WS Pro Proxy Agent, supported devices	28
Appendix B—HP Web Jetadmin support for telecommuter devices	30
HP Web Jetadmin best practices for managing telecommuter devices	30

OVERVIEW

Administrators want the ability to discover all the printing devices that are in use in order to evaluate their entire device inventory and move toward a balanced deployment. Devices that are directly connected to client machines on the network via USB and parallel (LPT) connections have always proven troublesome because it typically involves a physical inventory to locate them. Fortunately, HP Web Jetadmin provides two separate techniques for remotely discovering PC-connected devices that eliminate the need for physical inventories. One technique involves no client software, but can discover only the device model names, which might be useful for quickly determining inventory. The other technique involves installing client software, but can fully manage the devices by gathering many additional details beyond the model name.

PROXY AGENTS vs. WMI

HP Web Jetadmin provides the following methods for discovering devices directly connected to client machines:

- Windows® Management Instrumentation (WMI)
- Proxy agents (HP SNMP Proxy Agent and HP WS Pro Proxy Agent)

WMI is a set of extensions to the Windows Driver Model that provides an operating system interface through which instrumented components provide information and notifications. If administrator credentials are provided, HP Web Jetadmin can use WMI calls to discover directly connected devices. WMI calls can extract the plug-and-play ID of any directly connected device from the registry. WMI must be installed on all workstations. Administrator rights are required on the workstations to make the WMI calls. However, the only information about the device that WMI extracts is the model name. Discovered devices appear in the **All Devices** list along with the networked devices, but are distinguishable in the **Port** column as either **LPTx** or **USBxxx**.

The proxy agents are client-side software that allow HP Web Jetadmin to discover and manage directly connected devices. HP SNMP Proxy Agent works by exposing printer management information base (MIB) object identifiers (OIDs) to the Microsoft® SNMP service running on the client. HP WS Pro Proxy Agent is a WCF service running as a Network Service that resides on a PC workstation and replicates a device's services from the host computer's USB interface to its network interface. While most devices support HP SNMP Proxy Agent, a few require HP WS Pro Proxy Agent. Discovered devices appear in the **All Devices** list along with the networked devices, but are distinguishable in the **Port** column as **PC Port**. The client software is capable of passing the same types of questions to PC-connected devices that are typically passed to network-connected devices. Therefore, additional device information can be gathered, such as remaining toner levels, page counts, and status.

Comparison matrix

	Proxy agents	WMI
Credentials	Admin rights are required to install the agent on the client machines, but not to run discoveries.	Admin rights are required on all client machines to successfully discover PC-connected devices using WMI calls.
Client machines	The proxy agent must be installed on all client machines. The SNMP service must be active on client machines for the SNMP proxy.	WMI must be active on client machines.
Performance	Discoveries are much faster using simple SNMP requests or Web Services.	Discoveries that use WMI calls are slower.
Discoveries	Normal HP Web Jetadmin network device discovery techniques are used.	Normal HP Web Jetadmin network device discovery techniques are used.

	Proxy agents	WMI
Device List	PC-connected devices are distinguishable in the Port column as PC Port .	PC-connected devices are distinguishable in the Port column as LPTx or USBxxx .
Reports	Yes	Yes, but page counts are not collected, so reports can function only as inventory counts.
Model name	Accurately displays the model name of the device based on the gdStatusID object on the device or Web Service ticket.	Accurately displays the model name of the device based on the plug-and-play entry in the registry. This method is not completely reliable for LPT ports.
Status	Yes	No
Serial number	Yes, for devices that support the object	No
Page counts	Yes, for devices that support the object	No
Toner/ink levels	Yes, for devices that support the object	No
Alerts	Yes, using polling for status	No
Configuration	Yes, network setting prohibited	No

PROXY AGENTS

Proxy agents are designed for administrators who need not only the inventories of PC-connected devices but also the ability to manage them. Administrators who are willing to install client software reap the benefits of being able to extract additional device information, such as remaining toner levels, page counts, and status. Simple HP Web Jetadmin discoveries can also be performed to locate PC-connected devices without requiring administrator rights on those client machines.

Installation

The following modes of installation are available through standard tools, such as Microsoft Systems Management Server (SMS):

- Standalone installation—The standard (non-silent) installation that takes input from the user in the form of responses to dialog boxes. Administrators can install the package using an MSI package.
- Silent mode installation/network installation—The silent mode (without UI) is provided for push-based installations. Administrators can initiate a silent installation of the MSI package.

The following installation files are available for download:

- HP SNMP Proxy_32_10_4_0.msi (32-bit HP SNMP Proxy Agent installer)
- HP SNMP Proxy_64_10_4_0.msi (64-bit HP SNMP Proxy Agent installer)
- HPWSProxyService_10_3_8.exe (32-bit and 64-bit HP WS Pro Proxy Agent installer)

Silent mode installation—HP SNMP Proxy Agent

The HP SNMP Proxy Agent installer accepts the following command-line parameters in silent mode:

- /s
Silent extraction of the packaged binaries on the client system.
- /qn
Executes the MSI in silent mode. Just specifying /s implies this setting.
- /i
Indicates that the installer is used for installing the package.
- /fv
Indicates that the installer is used to upgrade an existing package.
- /x

Indicates that the installer is being used to uninstall an already installed package.

- `PERMITTEDMANAGERS="ipaddress1;ipaddress2;...;ipaddressn"`

This parameter sets up the SNMP service to respond only to requests from the specified IP addresses. An empty string, such as `PERMITTEDMANAGERS=""`, removes all existing entries that the proxy installer previously made. A value of "*" indicates that the SNMP service can receive values from any server.

- `VALIDCOMMUNITIES="communityname1;communityname2;...communitynamen"`

This parameter sets up the SNMP service to respond only to requests using one of the specified community names.

The following are examples of the typical usage:

1. To install the proxy in silent mode without making any additional entries or changes to the SNMP service:

```
hp_snmp_proxy.exe /s /i
```

2. To install the proxy in silent mode and set the allowed managers setting in the SNMP service:

```
hp_snmp_proxy.exe /s /I  
PERMITTEDMANAGERS="127.0.0.1;162.162.162.162;15.5.178.64"
```

3. To install the proxy in silent mode and set the allowed community names setting in the SNMP service:

```
hp_snmp_proxy.exe /s /i VALIDCOMMUNITIES="public;public.1;public.2"
```

4. To install the proxy in silent mode and set both the allowed community names and permitted managers setting in the SNMP service:

```
hp_snmp_proxy.exe /s /i  
PERMITTEDMANAGERS="127.0.0.1;162.162.162.162;15.5.178.64"  
VALIDCOMMUNITIES="public;public.1;public.2"
```

5. To modify the permitted managers or valid community names, use method 3 or 4, but specify /fv instead of /i.

6. To erase the permitted managers or valid community names, use method 3 or 4, but specify /fv instead of /i and specify PERMITTEDMANAGERS and/or VALIDCOMMUNITIES with the values set to "" (empty string).

7. To uninstall the proxy in silent mode:

```
hp_snmp_proxy.exe /s /x
```

Silent mode installation—HP WS Pro Proxy Agent

The HP WS Pro Proxy Agent installer accepts the following command-line parameters in silent mode:

- `WJAHOSTIP`

This parameter specifies the host IP of the HP Web Jetadmin server where HPWSProxyService sends WS Probe 'Hello' packets when the service is started and when it detects that the host machine has changed IP addresses. The intent is to keep the PC-connected device up-to-date in HP Web Jetadmin device lists without requiring another discovery.

default value: <not configured>

- WJADISCOVERYPORT

This parameter specifies the port where HPWSProxyService sends WS Probe 'Hello' packets. This port must be in sync with the port that HP Web Jetadmin is configured to listen on for PC-connect WS hello messages.

default value: 27893

- LEDMDISCOVERYPORT

This parameter specifies the port that HPWSProxyService listens on for discovery probe requests. Note that this is the UDP port. This port must be in sync with the port where HP Web Jetadmin is configured to send PC-connect WS probes.

default value: 27893

The following is an examples of the command-line command:

```
msiexec /i HPWSProxyService.msi WJAHOSTIP=1.2.3.4
WJADISCOVERYPORT=27893 LEDMDISCOVERYPORT=27893
```

HP SNMP Proxy Agent

HP SNMP Proxy Agent implements its service as an *Extension Agent* within the framework provided by Microsoft SNMP Service for Windows. Therefore, HP SNMP Proxy Agent requires that Microsoft SNMP Service already be installed. The proxy uses a *redirector* to multiplex multiple devices through a single host IP address.

The proxy's extension agent implements the following SNMP MIBs:

- HP proprietary Printer Management Language (PML) MIB.
- Standard Printer (STD) MIB
- HP Jetdirect (NP) MIB beneath the HP Enterprise MIB
- HP SNMP Proxy Agent MIB beneath the HP Enterprise MIB

The Microsoft SNMP Service component for Windows implements the following MIBs:

- MIB-II
- Host Resource (HR) MIB

Microsoft organizes the *hrDeviceStatus*, *hrPrinterStatus* and *hrPrinterDetectedErrorState* tables differently than HP Jetdirect. Because these tables include many devices (such as mice, CD-ROMs, keyboards, and disks) as well as zero or one or more printers, HP Web Jetadmin uses the proxy's *redirector* for accessing the device's host resource MIB.

Unredirected queries about the network interface (IP address, subnet mask, and so on) query the corresponding tables in the Windows Workstation, not the device (even if the device is also networked). To access MIB-II in the device, HP Web Jetadmin must use the *redirector*.

HP WS Pro Proxy Agent

Newer HP devices support management protocols more advanced than SNMP that use Web Services, namely WS* and LEDM. HP WS Pro Proxy Agent was developed to support LEDM printers that do not support enough of SNMP for HP SNMP Proxy Agent to provide the desired management. HP WS Pro Proxy Agent resides on a PC workstation and replicates a device's services from the host computer's USB interface to its network interface. HP SNMP Proxy Agent runs as a Network Service when installed on workstations and is developed using WCF 4.0 to leverage the WS-Discovery feature. Microsoft .NET Framework 4.0 is required for installation. Each HP Web Jetadmin installation

contains an HP WS Pro Adapter that handles the mappings between WS* and LEDM tickets. The HP WS Pro Adapter service must be running on the HP Web Jetadmin server to discover and manage devices through HP WS Pro Proxy Agent.

HP WS Pro Proxy Agent is not a WS* proxy. While LEDM and WS* devices share two services—the WS-Discovery service and the WS-Transfer device service—most traffic is different. LEDM device management traffic is RESTful with a URL for each *ticket*. WS-Management traffic is SOAP-based with a URL for each service.

HP WS Pro Proxy Agent gains access to the USB-connected printer through a component of the Printer Driver known as UIO. The printer information exposed to HP WS Pro Proxy Agent via Web Services is plentiful, providing an opportunity for strong management capabilities of these devices.

DISCOVERY

HP Web Jetadmin can perform discoveries for either networked devices or PC-connected devices. A discovery for PC-connected devices always begins by scanning the network to find active nodes. An active node is any networked device that responds to the discovery method that HP Web Jetadmin uses. Figure 1 shows the supported discovery methods that can be used to locate nodes containing locally connected devices. The following are the most common techniques:

- **IP range**—Sends SNMP query packets to all addresses in the specified IP address ranges of.
- **Specified address**—Sends SNMP query packets to only the IP addresses specified in the list.

Note Quick Device Discovery on the main HP Web Jetadmin page is not supported for discovering PC-connected devices. Quick Device Discovery is intended to find only network-connected devices. PC-connected discoveries require a different technique than network-connected discoveries. Quick Device Discovery cannot discard workstations. Quick Device Discovery must continue probing to determine if a proxy is installed and which port on the workstation contains a printer.

Remember, HP Web Jetadmin queries workstations instead of devices, so take care to ensure that accurate ranges or lists of IP addresses are defined.

After the node portion of the discovery is complete, HP Web Jetadmin begins a resolution process to qualify either PC-connected devices or network-connected devices. HP Web Jetadmin interrogates each node with SNMP queries to determine if the node has any proxy agents installed.

If it is determined that HP WS Pro Proxy Agent is installed, HP Web Jetadmin attempts to talk to any USB-connected devices through the HP WS Pro Proxy Agent service that was installed when the proxy was installed. All the calls to the USB devices are routed through the HP Web WS Pro Adaptor

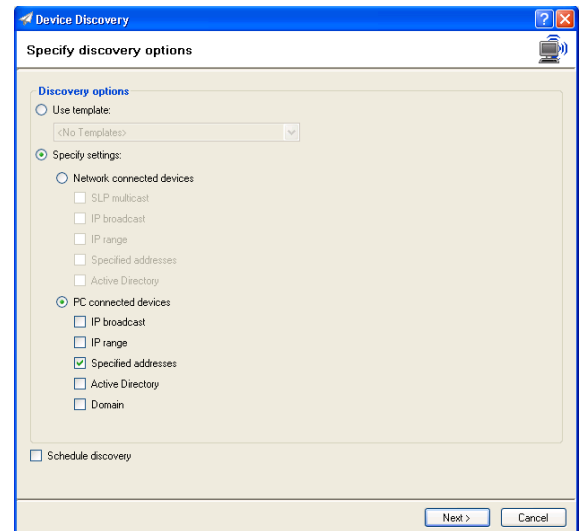


Figure 1—Discovery methods

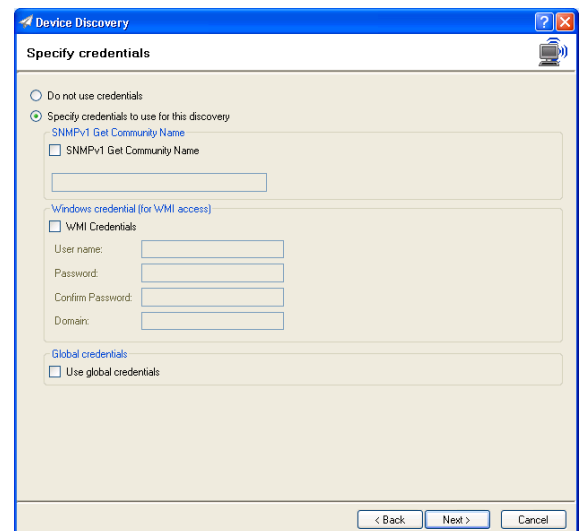
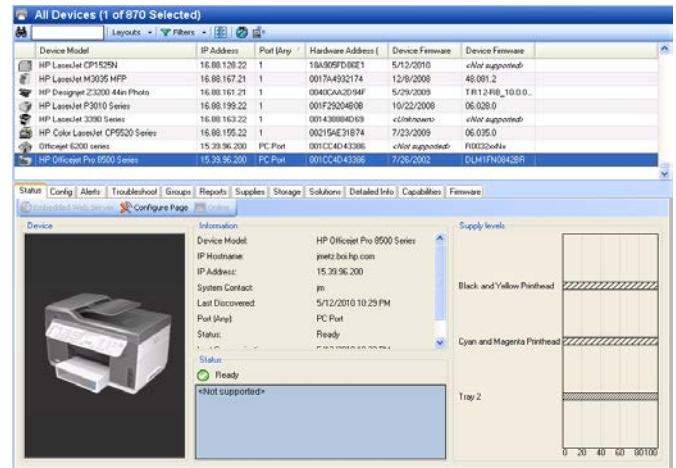


Figure 2—WMI Credentials

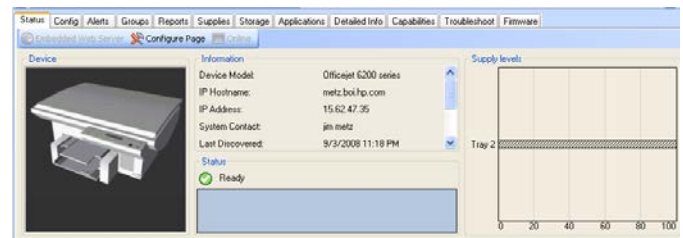
service running on the HP Web Jetadmin server, which acts as an interface between the HP Web Jetadmin and HP WS Pro Proxy services.

If it is determined that HP SNMP Proxy Agent is installed, additional standard printer and enterprise PML OIDs are queried to determine if a supported device is connected. The proxy filters these OIDs and redirects them to the device over the USB or LPT cable. Other OIDs, such as Host Resources objects, are passed through to the SNMP service so that the workstation can provide responses pertaining to itself. This is imperative for using enterprise management solutions to manage client machines. When queries are passed to the device, in most cases the device model name, engine page count, toner levels, serial number, and more are available.



Device Model	IP Address	Port (Any)	Hardware Address	Device Firmware	Device Firmware
HP LaserJet CP1525N	16.88.128.22	1	18A369FD08E1	5/12/2010	<Not supported>
HP LaserJet M3025 MFP	16.88.167.21	1	0017A4932174	12/8/2008	48.081.2
HP DesignJet Z3200 44in Photo	16.88.167.21	1	0040CAA2D94F	5/29/2009	1 R12-Rev_10.0.0.
HP LaserJet P3010 Series	16.88.199.22	1	001F26204808	10/22/2008	06.028.0
HP LaserJet 3200 Series	16.88.183.22	1	001438984D93	<Unknown>	<Not supported>
HP Color LaserJet CP9520 Series	16.88.195.22	1	002194E31874	7/23/2009	06.035.0
Officejet G200 series	15.29.96.200	PC Port	001CC4D43396	<Not supported>	00033004a
HP Officejet Pro 8500 Series	15.29.96.200	PC Port	001CC4D43396	7/26/2002	04M1FN0342BR

Figure 3—Devices discovered by HP SNMP Proxy Agent



Information	Value
Device Model	HP Officejet Pro 8500 Series
IP Hostname	metz.boi.hp.com
IP Address	15.29.96.200
System Contact	jim
Last Discovered	5/12/2010 10:29 PM
Port (Any)	PC Port
Status	Ready
Not supported	

Figure 4—Status tab

If it is determined that neither proxy is installed or if no device can be found on machines where a proxy is installed, HP Web Jetadmin then attempts to locate devices using WMI if the **WMI Credentials** checkbox is selected (Figure 2). The credentials entered **must** be a member of the administrator's group on any workstation for HP Web Jetadmin to perform WMI calls to discover PC-connected devices.

Printers discovered using either proxy agent are displayed in the **All Devices** list with **PC Port** in the **Port** column (Figure 3). Devices discovered using WMI are displayed in the **All Devices** list with **LPTx** or **USBxxx** in the **Port** column. Multiple devices attached to a single workstation can be discovered. Each of the multiplexed devices on a PC have the same IP address, but have different HP Jetdirect port numbers—similar to the behavior of a multiport HP Jetdirect EX print server.

Note There are a handful of devices that by both HP SNMP Proxy Agent and HP WS Pro Proxy Agent can discover. If the latest versions of both proxies are installed and both proxies discover one of these devices, the device appears in the device lists only once as being discovered by HP WS Pro Proxy Agent. If older versions of the proxies are installed and both proxies discover one of these devices, the device appears in the device lists twice. The difference is noted by the type of information that is displayed by each proxy. For more information, see "Proxy comparison" on page 2.

DEVICE MANAGEMENT

The proxies can provide the following types of functionality for discovered devices:

- Display device information, such as status, supplies levels, and page counts
- Configure specific features
- Monitor device alerts
- Generate reports

The level of support for each device depends on the following variables:

- Which proxy discovered the device
- How the feature is exposed on the device
- How HP Web Jetadmin is defined to retrieve or configure the feature

View device information

Selecting a device that the proxies discovered in the **All Devices** list and selecting the **Status** tab displays various device details (Figure 4). Information such as **IP Address**, **IP Hostname**, and

Hardware Address pertain to the client workstation where the device is connected. The remaining details pertain to the device itself. A matching picture is displayed, including the real-time status of the device. Supply level gauges appear as well as descriptive items, including **Device Location** and **System Contact**. Again, all of this information depends on which proxy discovered the device and how HP Web Jetadmin is defined to support the feature.

Additional information pertaining to the device can be obtained by adding any of the hundreds of columns that are available. Items such as **Device Firmware Version**, **Engine Cycle Count**, **Serial Number**, and **Install Date** can be viewed in columns, just for starters.

Note Firmware upgrades for USB-connected devices and HP SNMP Proxy Agent or HP WS Pro Proxy Agent is not tested or supported.

If WMI discovered the device, no additional device information can be displayed on the **Status** tab other than the model name. Additional information is not available in the registry. Only the proxy agents can gather such information.

Set device configurations

Selecting a device that the proxy agents discovered in the **All Devices** list and selecting the **Config** tab displays various configuration options (Figure 5). The ability to set configuration items for printers discovered through HP SNMP Proxy Agent depends on the following factors:

- The SNMP service must be configured to allow for getting and setting information via SNMP. Right-click **SNMP Service**, select the **Security** tab, and edit the public community name to allow for **READ WRITE** community rights instead of the default value of **READ ONLY** (Figure 6).
- Only configuration items that use SNMP Set Request packets to configure are successful if discovered via HP SNMP Proxy Agent. Other settings that require HTTP packets to configure the device will fail. HP SNMP Proxy Agent only knows how to pass SNMP to the device.
- Only those SNMP configuration items that use OIDs defined in the standard printer MIB or the HP proprietary MIB are successful when using HP SNMP Proxy Agent. Configuration items that use MIB-II or Host

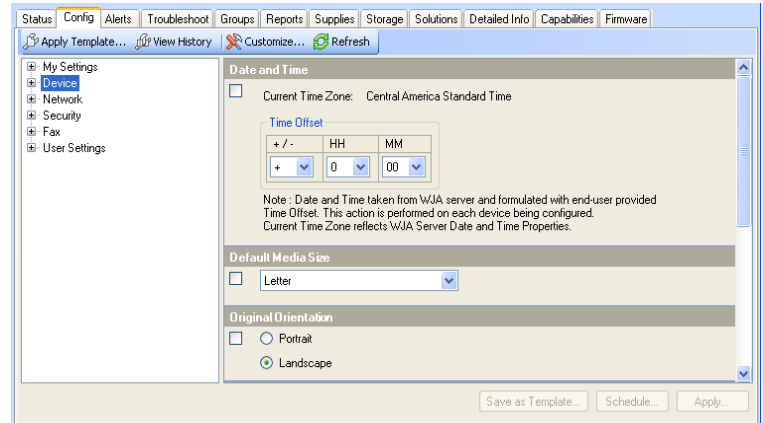


Figure 5—Device configuration

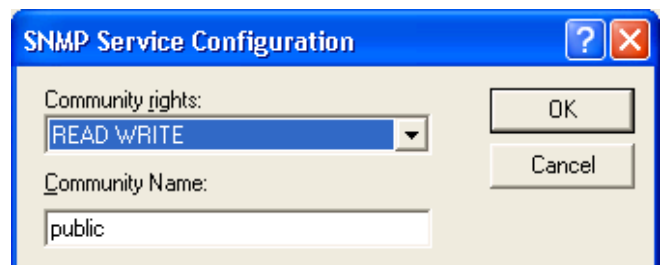


Figure 6—SNMP Service Configuration

Resources MIB are blocked because the PC might also support those OIDs. HP SNMP Proxy Agent directs on top of the SNMP service. HP SNMP Proxy Agent redirects objects intended for the device to the device and objects intended for the PC to the PC. For security reasons, HP SNMP Proxy Agent must block configuration SNMP Set Request packets that might apply to the PC, such as those found in MIB-II and Host Resources MIB. Items under **Networking** fail because they are set on the PC. The following are examples of the configuration items that are blocked:

- SNMP Trap Table
- System Contact
- System Location
- Set Community Name
- Get Community Name
- The devices that HP WS Pro Proxy Agent discover do not have restrictions between configuration items applying to the PC or printer because the PC does not support the Web Services calls.

Alerts

It is possible to monitor device alerts through the proxies. However, the number of alerts that can be monitored are limited to only the alerts that polling supports. HP Web Jetadmin cannot process traps through the proxies. Therefore, the alerts in the General category that use traps are not supported.

Reports

If the proxy discovers devices that display supply levels and page counts, the devices can be added to Data Collections and reports can be generated on the data that is collected.

PROXY COMPARISON

Recall earlier it was stated that the level of support for each device depends on the following variables:

- Which proxy discovered the device
- How the feature is exposed on the device
- How HP Web Jetadmin is defined to retrieve or configure the feature

HP Web Jetadmin can use a variety of techniques to retrieve or configure information, such as SNMP, DSMP, XDM, LEDM, and WS*. HP Web Jetadmin uses only one technique to support each feature on a specific device. If a device supports LEDM and a feature is exposed via LEDM, HP Web Jetadmin supports the feature using only LEDM for that device. Even if the device also exposes the feature through SNMP, HP Web Jetadmin uses the preferred technique of LEDM. This plays an important role in what each proxy supports on a given device.

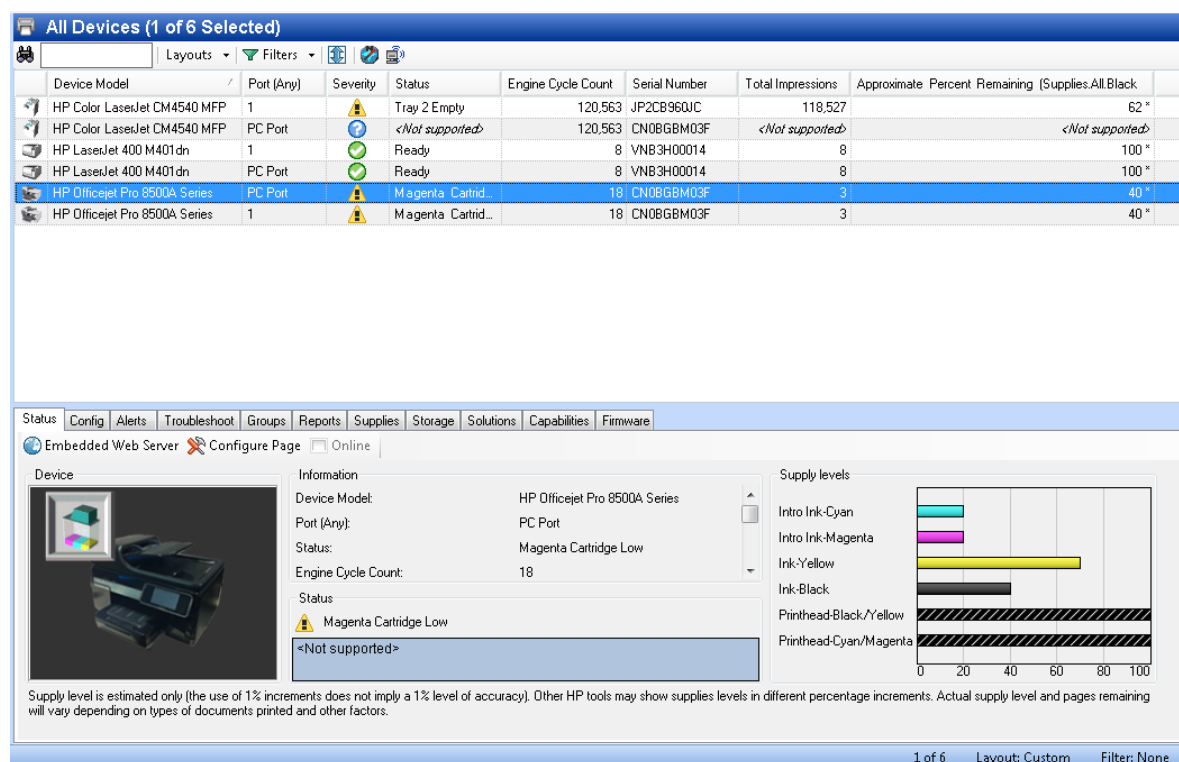
If HP SNMP Proxy Agent discovers the device, it exposes only the features that HP Web Jetadmin uses SNMP to support on that device. If HP WS Pro Proxy Agent discovers a device, it exposes only the features that HP Web Jetadmin uses LEDM to support on that device.

For example, the HP LaserJet 400 M401 device supports both SNMP and LEDM. Each feature is supported using only one technique. If a feature is exposed through LEDM, HP Web Jetadmin uses LEDM, regardless of whether the feature is also exposed through SNMP. It does not matter which proxy discovers the device. HP Web Jetadmin uses only LEDM for those features. This means that if HP SNMP Proxy Agent discovers the device, most features are not supported because HP Web Jetadmin must use LEDM.

Some items, such as Tray levels, are exposed only on LEDM devices through SNMP. This means that only HP SNMP Proxy Agent can display these items. HP WS Pro Proxy Agent cannot. There are very few items on LEDM devices that are exposed only via SNMP, making HP WS Pro Proxy Agent the preferred choice to discover and manage LEDM devices.

HP FutureSmart printers expose features through a Web Services protocol called WS*, but many features are also exposed through SNMP. However, HP Web Jetadmin is coded to use WS* if it is available for all features. HP WS Pro Proxy Agent cannot discover HP FutureSmart devices at all. While HP SNMP Proxy Agent can discover HP FutureSmart devices, it only displays the model name because HP Web Jetadmin must use WS* for everything else and HP SNMP Proxy Agent cannot pass WS*.

For examples of LEDM and HP FutureSmart printers, see “Supported devices” on page 11.



Comparisons of networked vs. PC-connected for SNMP, LEDM and WS* based printers

SUPPORTED DEVICES

WMI

A device can be discovered via WMI as long as the device supports plug-and-play and bi-directional communication has been established, which allows the device's plug-and-play ID to be placed into the registry. Both HP and third-party devices can be discovered via WMI. In fact, the printer driver is irrelevant in this case because the plug-and-play ID—not the driver name—is displayed as the model of the discovered device. The plug-and-play ID represents the physically connected device no matter which driver is used. Devices connected via LPT ports can pose a slight problem because the plug-and-play ID is only added or removed from the registry after a workstation power cycle.

HP SNMP Proxy Agent

HP SNMP Proxy Agent supports a wide variety of SNMP-capable HP devices that are directly connected to client machines and meet the following criteria:

- The Windows SNMP service must be installed and configured to allow queries from the HP Web Jetadmin server. The community name should be set to public for read access.
- Firewall settings must be appropriately modified to allow HP Web Jetadmin to query HP SNMP Proxy Agent. This means that UDP port 161 should be open for SNMP queries.
- Printers must be installed using a DOT4 bi-directional capable driver or a driver containing a special language monitor in order to respond to SNMP queries

For directly connected devices to be discovered via HP SNMP Proxy Agent, proper communication between the device and client machine must be provided. For devices that support DOT4, use a driver that provides an HP DOT4 port connection, whether the connection is via USB or LPT. An example of the correct port type is DOT4_001. If the port type is different (for instance, LPT1 or USB001), the following options can provide a proper DOT4-capable driver:

- Use HP Universal Print Driver (UPD) version 4.5 or later.
- When using HP Universal Print Driver (UPD) 6.1 or later, HP SNMP Proxy 10.4 or later is required.
- Use the HP printing system software CD that came with the device to install the HP DOT4 port.
- If the printing system software CD is not available, download the latest printing system software from www.hp.com.

Composite USB devices that do not support DOT4, such as the HP LaserJet P2055 printer, require a language monitor that is capable of passing PML over Printer Job Language (PJI). HP UPD 4.7 added support for composite USB devices.

A complete list of printers supported by UPD can be found on the HP UPD website. For a complete list of tested devices, see “Appendix A—Supported printing devices” on page 26. Items in yellow indicate LEDM devices that provide very little information if HP SNMP Proxy Agent discovers them. Items in red indicate HP FutureSmart devices that provide nothing more than the model name using HP SNMP Proxy Agent.

HP WS Pro Proxy Agent

HP WS Pro Proxy Agent requires that .NET Framework 4.0 be installed. HP WS Pro Proxy Agent installs as its own service and does not require the Microsoft SNMP service to be installed. This proxy discovers devices that support LEDM, which is a special form of Web Services for communication.

For a complete list of tested and supported devices, see “Appendix A—Supported printing devices” on page 26.

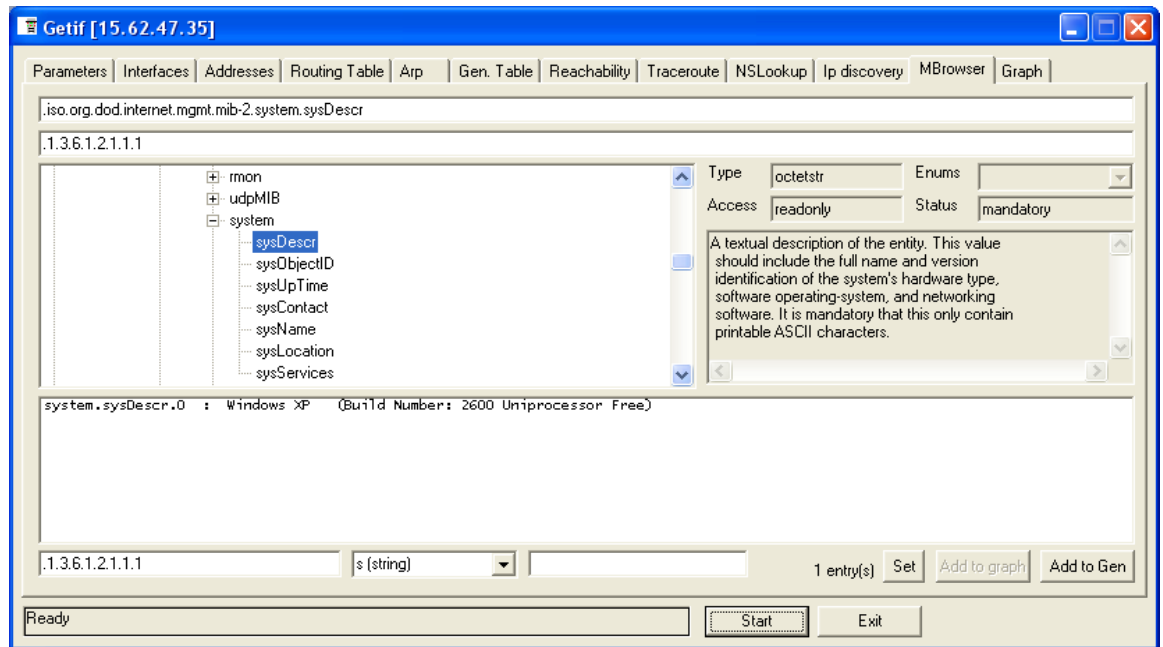
TROUBLESHOOTING DISCOVERY

HP SNMP Proxy Agent

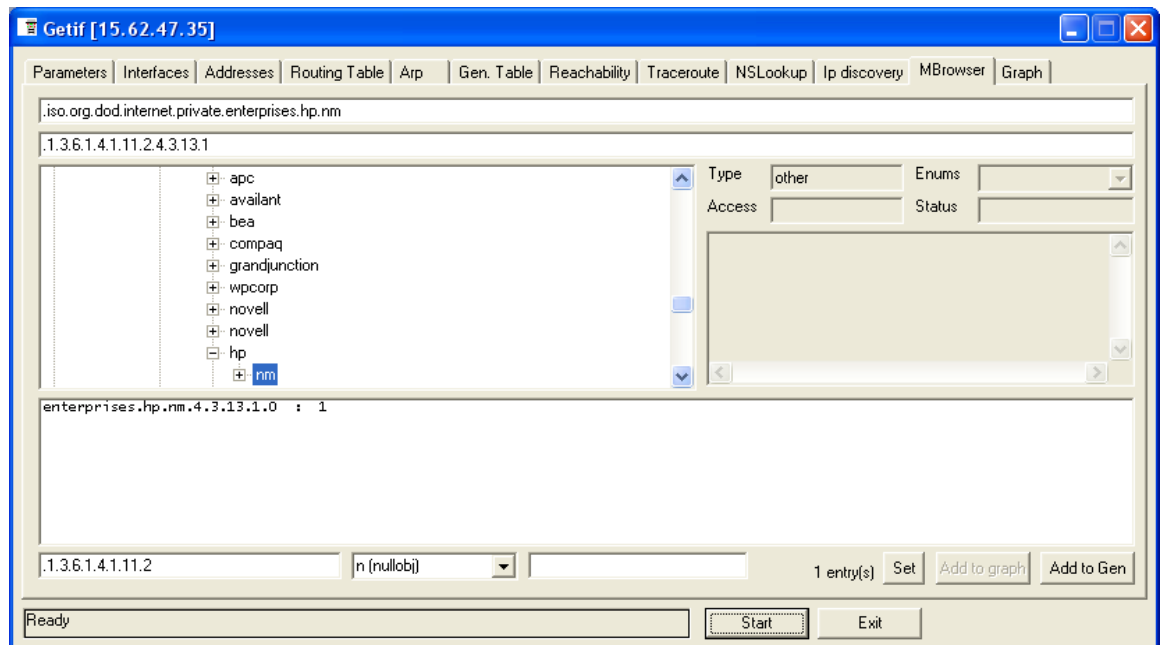
If HP Web Jetadmin does not discover PC-connected devices running HP SNMP Proxy Agent or HP WS Pro Proxy Agent, try the following troubleshooting steps to understand why the discovery fails. The key to these issues is proving that the communication channel between HP Web Jetadmin and the proxy is working, and then focusing on the printer driver as the culprit.

1. HP SNMP Proxy Agent or HP WS Pro Proxy Agent must be installed on the client computers. Check the version to make sure it is the latest version available on the Web. HP SNMP Proxy Agent appears as a program under Add/Remove Programs. HP WS Pro Proxy Agent appears as a service that must be running.
2. The Microsoft SNMP service, which is a Windows Component and a service, must be installed and started on the client computers for HP SNMP Proxy Agent to discover devices. The SNMP Proxy Agent installer will not complete without the SNMP service running. However, the SNMP service might have been removed or stopped after the proxy was installed.
3. The Microsoft SNMP service must be configured to provide HP Web Jetadmin with read access through a mutually agreed-upon community name, such as public.
4. The Microsoft SNMP service must be configured to grant access to either the management application's host IP address or all IP addresses.
5. The client computers must be equipped with a supported HP device. For a list of supported devices, see "Appendix A—Supported printing devices" on page 26.
6. The printer driver must be installed with a supported bi-directional I/O stack. An easy way to ensure this is to install HP UPD or a printing system driver that provides a DOT4 port. There are no guarantees that the latest or largest driver obtained on the Web contains the DOT4 bi-directional stack, but the chances are better. HP UPD also provides the necessary language monitor for composite devices, such as the HP LaserJet P2055.
7. Firewalls on client computers must be configured to pass traffic on UDP port 161 (SNMP).
8. Verify basic network connectivity by pinging the client machine from the HP Web Jetadmin server.
9. Use a third-party SNMP tool, such as SNMP Get or GetIf, to verify basic SNMP service on the Windows client. Any tool capable of gathering SNMP information should suffice. A typically supported object to query in order to prove SNMP communication is 1.3.6.1.2.1.1.1 (sysDescr). For example:

```
snmpget -v 2c -c public clienthostname 1.3.6.1.2.1.1.1
```



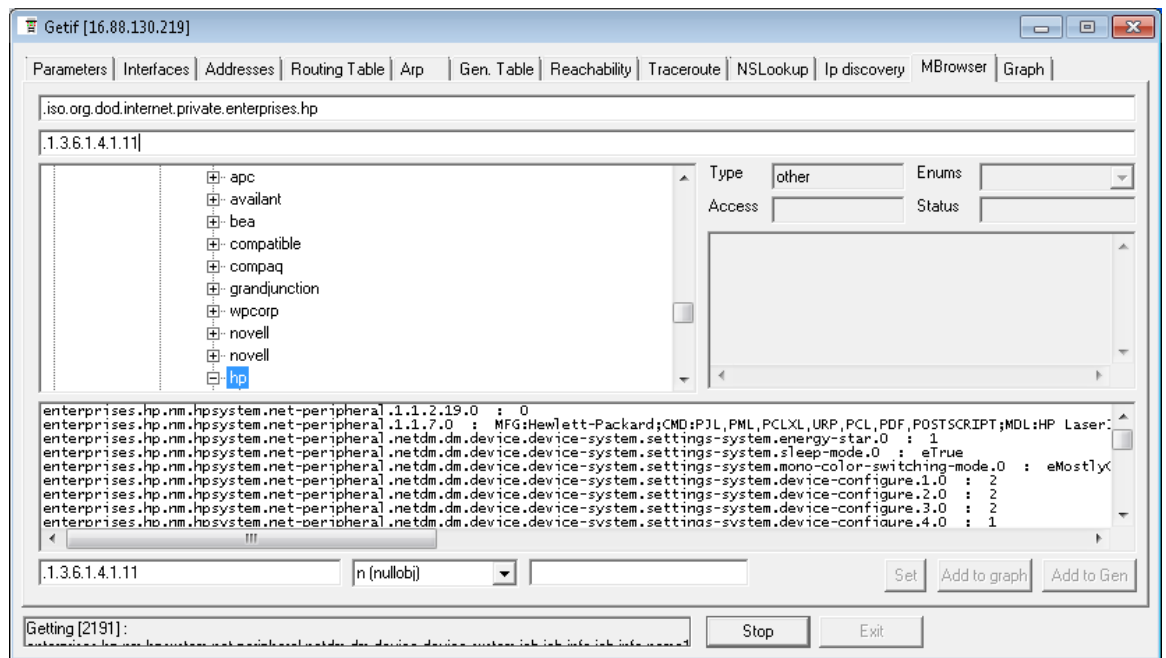
10. Use a third-party SNMP tool, such as SNMP Get or GetIF, to verify the successful installation of HP SNMP Proxy Agent. To prove a successful installation of the proxy, query 1.3.6.1.4.1.11.2.4.3.13.1.0. If the agent, printer driver, and device are all functioning, the agent responds with an INTEGER such as "1". If the agent is installed and configured correctly, but unable to communicate with the device, the agent responds with the error "NO SUCH NAME".



Using Getif to prove a successful HP SNMP Proxy Agent installation

11. If SNMP communication is proven to work, it is possible that the printer driver does not allow the redirector to pass SNMP queries on to the printer or the device is LEDM and does not support enough of SNMP. Use the same SNMP tool to determine if the machine with the proxy can walk the PML MIB starting with the following OID:

.1.3.6.1.4.1.11

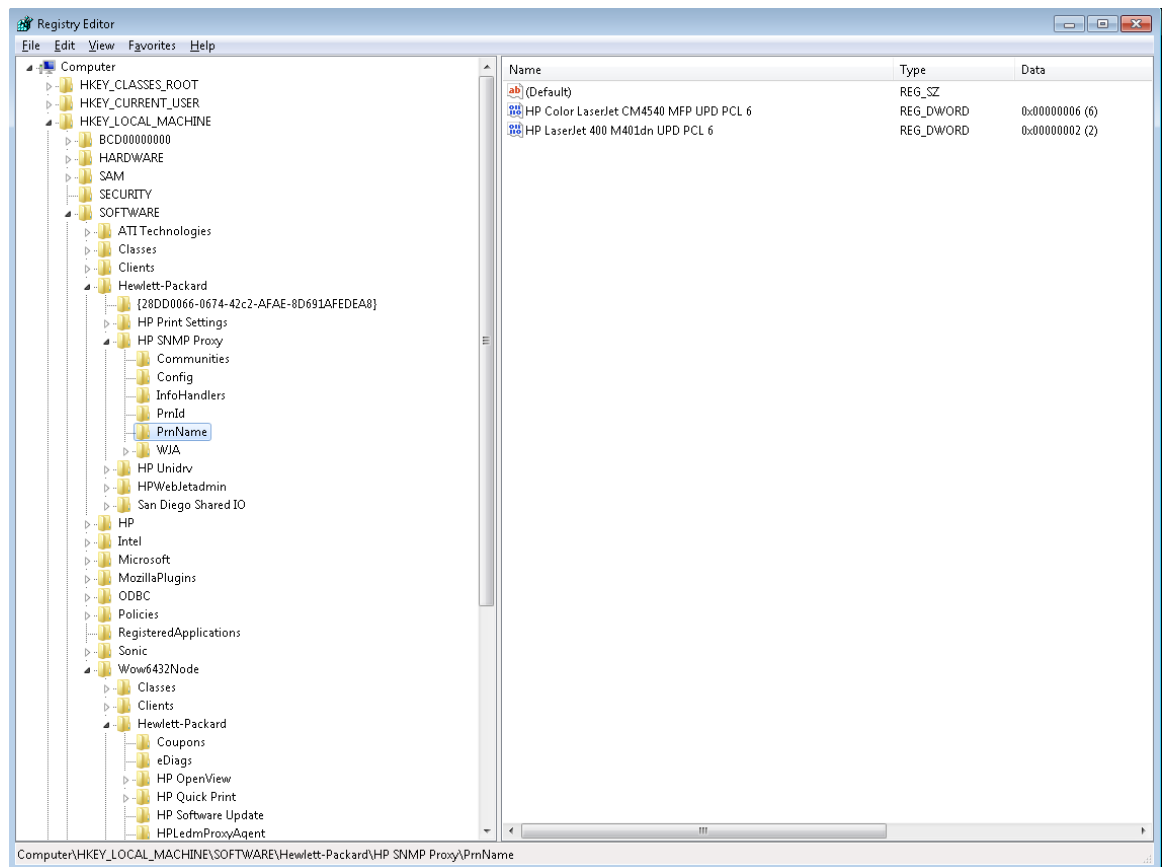


If the machine responds with answers to many OIDS, it is very likely that discoveries are successfully occurring. If only a few OIDs respond, the problem is likely that the installed printer/scanner driver does not expose the necessary device management interface (PML) to HP SNMP Proxy Agent.

12. Drivers are a common source of problems. Assuming that the printer is supported, but full SNMP communication fails, browse to the following registry entry on the desktop PC:

\HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\HP SNMP Proxy\PrnId

This registry entry records the name of the instrumented printer/scanner drivers, if any. If the PC's printer/scanner is supported, but the proxy cannot instrument its driver, the PC requires a different printer/scanner driver.



13. If the installed printer is connected to a parallel port, but Windows is unable to use bi-directional communication with the device, check to see if either the PC's BIOS is misconfigured or the parallel cable does not support bi-directional communication. Setting the parallel port to use ECP in the BIOS setup might solve the problem.

HP WS Pro Proxy Agent

1. Verify that the HPWSProxy service is using port 27893. Open a Windows command window, and issue the following command:

```
netstat -a -b
```

In the returned list, you should find the following:

```
UDP        0.0.0.0:27893          *.*          [HPDeviceProxyService.exe]
```

Alternatively, double-click the HP Device Proxy Console App file, and verify that there is no exception. This file is available in the following locations:

- For 32-bit OSes:
C:\Program Files\Hewlett-Packard Company\HPWSProxy\HPWSProxy\bin
- For 64-bit OSes:
C:\Program Files (x86)\Hewlett-Packard Company\HPWSProxy\HPWSProxy\bin

If HP WS Pro Proxy Agent is installed on the same machine as HP Web Jetadmin and PC-connected discoveries are run through HP Web Jetadmin, there is a conflict because both want to use port 27893.

2. Verify that the LEDM endpoints are hosted by the device. Open the HPWSProxyService.log file, which is available in the same location as the HP Device Proxy Console App provided in issue 1. Find entries that contain the endpoint verbiage, such as the following:
 Hosted Endpoints are
 https://IPAdress:8022/434E434A-3230-3030-3735-2C768A3EB978
 http://IPAdress:8023/434E434A-3230-3030-3735-2C768A3EB978/transfer
3. If no Hosted Endpoints are listed in the log file, check for errors, such as the following:
 Exception caught in the function OnReceiveRequest...Object reference not set to an instance of an object.
 If this error is listed, the proxy agent cannot connect to the printer. It is likely that another application is using the socket connection that HP WS Proxy Agent needs. This might mean that VMware Workstation is installed on the same client as HP WS Proxy Agent.
4. Verify that the latest version of HP WS Pro Proxy Agent is installed. The version is displayed in the **Name** and **Version** columns in **Control Panel > Program and Features**. Versions prior to HP WS Pro Proxy Agent 10.3.1 display only the version in the **Version** column or might not display any version at all.

DISCOVERY LOGS

Additional log file functionality that allows administrators to understand and troubleshoot PC-connected device discoveries is available in HP Web Jetadmin. The following sections provide instructions for enabling and gathering the logging details for HP SNMP Proxy Agent, HP WS Pro Proxy Agent, and WML.

PC-connected discovery logging in HP Web Jetadmin

1. Use Microsoft Notepad or a similar editor to open the following file:
 C:\Windows\ServiceProfiles\NetworkService\AppData\Local\HP
 Inc\HPWebJetadmin\Settings\WjaService\config\DiscoveryManager.config.xml
2. Find the following section:

```
<property name="DiscoveryLogEnabled">
  <type>HP.Imaging.Wjp.Sdk.Core.Framework.ConfigurationItemString
  </type>
  <value>False</value>
</property>
```
3. Change the <value> entry as follows:

```
<property name="DiscoveryLogEnabled">
  <type>HP.Imaging.Wjp.Sdk.Core.Framework.ConfigurationItemString
  </type>
  <value>True</value>
</property>
```
4. Save the file.

Additional settings can be used to increase the number of log files that the system creates. The default setting instructs the system to overwrite a second log file for each new discovery.

1. Use Notepad or a similar editor to open the following file:
 C:\Documents and Settings\NetworkService\Local Settings\Application Data\HP
 Inc\HPWebJetadmin\WjaService\config\DiscoveryManager.config.xml

2. Find the following section:

```
<property name="NumDiscoveryLogs">
  <type>HP.Imaging.Wjp.Sdk.Core.Framework.ConfigurationItemString
</type>
  <value>2</value>
</property>
```

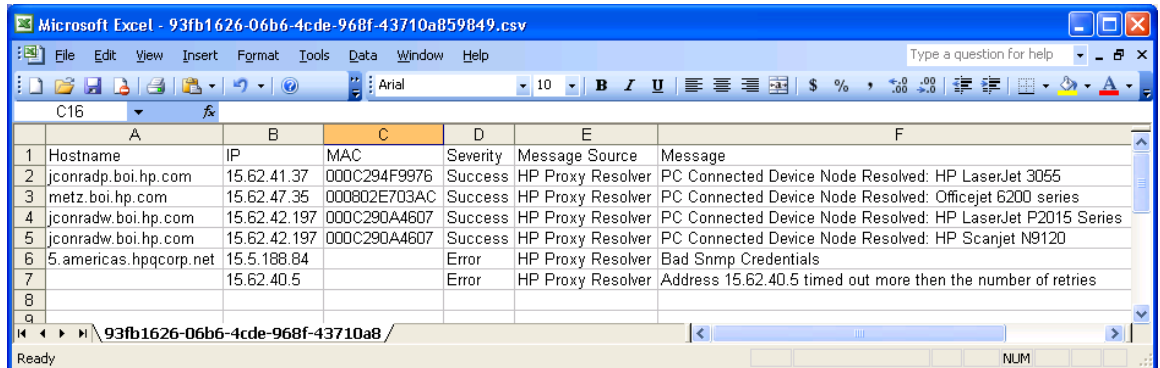
3. Change the <value> entry to the required number of log files.

4. Restart the HP Web Jetadmin service (HP WJA Service).

After discovery logging is enabled, PC-connected device discoveries add entries to the log files that are available in the following directory:

C:\Documents and Settings\NetworkService\Local Settings\Application Data\HP
Inc\HPWebJetadmin\WjaService\DiscoveryLog

Each time HP Web Jetadmin contacts an address to determine the presence of a PC-connected device, it adds an entry to this log (Figure 7). Log entries indicate which method of discovery was attempted (HP SNMP Proxy Agent vs. WMI) and the result (such as no SNMP response, bad WMI credentials, and discovered devices).



	A	B	C	D	E	F
	Hostname	IP	MAC	Severity	Message Source	Message
1						
2	jconradp.boi.hp.com	15.62.41.37	000C294F9976	Success	HP Proxy Resolver	PC Connected Device Node Resolved: HP LaserJet 3055
3	metz.boi.hp.com	15.62.47.35	000802E703AC	Success	HP Proxy Resolver	PC Connected Device Node Resolved: Officejet 6200 series
4	jconradw.boi.hp.com	15.62.42.197	000C290A4607	Success	HP Proxy Resolver	PC Connected Device Node Resolved: HP LaserJet P2015 Series
5	jconradw.boi.hp.com	15.62.42.197	000C290A4607	Success	HP Proxy Resolver	PC Connected Device Node Resolved: HP Scanjet N9120
6	5.americas.hpqcorp.net	15.5.188.84		Error	HP Proxy Resolver	Bad Snmp Credentials
7		15.62.40.5		Error	HP Proxy Resolver	Address 15.62.40.5 timed out more then the number of retries
8						
9						

Figure 7—Discovery logging

Error logging and troubleshooting HPWS Proxy Agent

Change the settings in the ProxyService.config.xml file.

The settings in the ProxyService.config.xml file determine the behavior of HP WS Pro Proxy Agent. The ProxyService.config.xml file and the corresponding log files (HPWSProxyServiceLog.log and DeviceManager.log) are located in one of the following directories:

- On a 32-bit operating system:

C:\Program Files\HP Inc\HPWSProxy\bin\

- On a 64-bit operating system:

C:\Program Files (x86)\Hewlett-Packard Company\HPWSProxy\bin\

Note HP WS Pro Proxy Agent 10.3.8 and earlier, these files are located in one of the following directories:

- On a 32-bit operating system:

C:\Program Files\Hewlett-Packard Company\HPWSProxy\bin\

- On a 64-bit operating system:

C:\Program Files (x86)\Hewlett-Packard Company\HPWSProxy\bin\

Validate whether HPWSProxyService can communicate with a USB-connected printer

If the HPWSProxyServiceLog.log file contains endpoints, the proxy server can communicate with a USB-connected device. The following is an example of an endpoint in the log:

```
ProcessID:1944, Time:6/14/2016 6:26:58 PM, MustWrite] Hosted Endpoints  
are[ProcessID:1944, Time:6/14/2016 6:26:58 PM, MustWrite]  
https://10.10.10.20:8020/564E4333-4230-3032-3538-  
308D99AD1AE6[ProcessID:1944, Time:6/14/2016 6:26:58 PM, MustWrite]  
http://10.10.10.20:8021/564E4333-4230-3032-3538-308D99AD1AE6/transfer
```

Validate whether remote communication with an LEDM USB-connected printer outside of HP Web Jetadmin is possible

To test whether the endpoint of an LEDM device in the example in the previous section is accessible via the network, add /DevMgmt/ProductConfigDyn.xml to the URL. From the example in the previous section, use the following URL in a web browser to test the endpoint:

```
https://10.10.10.20:8020/564E4333-4230-3032-3538-  
308D99AD1AE6/DevMgmt/ProductConfigDyn.xml
```

A user name and password are requested. The user name and password must be for a user who has access to the PC to which the device is connected. For this example, the PC has an IP address of 10.10.10.20. If no data is displayed, the network is blocking the traffic or HPWSProxyService has been stopped.

The endpoint contains the device UUID that the printer generates. The last digits of the UUID are the MAC address of the printer.

Default ProxyService.config.xml file

```
<?xml version="1.0" encoding="utf-8"?>
<ProxyServiceConfig>
  <SimulatedMode>false</SimulatedMode>
  <UseAug2004Addressing>true</UseAug2004Addressing>
  <EnableHTTPS>true</EnableHTTPS>
  <!-- Log levels are : Error, Message, Warning, All -->
  <LogLevel>Error</LogLevel>
  <DefaultRegistryPath>SOFTWARE\Wow6432Node\Hewlett-Packard
\HPLedmProxyAgent</DefaultRegistryPath>
  <RegistryPath>SOFTWARE\Hewlett-Packard\HPLedmProxyAgent</RegistryPath>
  <RegistryPathToGetWJAHostIP>SOFTWARE\Hewlett-Packard\HPLedmProxyAgent</
RegistryPathToGetWJAHostIP>
  <EnableTestingIPAddressChange>false</EnableTestingIPAddressChange>
  <DefaultPort>8082</DefaultPort>
  <DefaultWSTransferPort>8083</DefaultWSTransferPort>
  <AssignedPort>8020</AssignedPort>
  <EnableCustomDiscovery>true</EnableCustomDiscovery>
  <UIOVersion>2.0.0.533</UIOVersion>
  <EnableActiveDeviceDetection>true</EnableActiveDeviceDetection>
  <!-- Extra Debug Settings -->
  <LogDetectedPrinterInfo>false</LogDetectedPrinterInfo>
  <LogLedmAdapterClientIPLogging>false</LogLedmAdapterClientIPLogging>
</ProxyServiceConfig>
```

- **LogLevel** (all versions of HP WS Pro Proxy Agent)

The default log level is Error. To change the log level, edit the ProxyService.config.xml file in one of the directories listed previously. After the log level is changed, HPWSProxyService must be restarted.

If the log level is set to All, HPWSProxyService creates a second log file called DeviceManager.log.

- **EnableActiveDeviceDetection** (HP WS Pro Proxy Agent 10.4.1 and later)

The default value is true. HPWSProxyService actively checks to detect whether printers are attached to the PC. This functionality is new in HP WS Pro Proxy Agent 10.4.1. Earlier versions of HP WS Pro Proxy Agent use only passive listening for Windows event to detect newly attached printers.

The following is an example of a log message:

```
[ProcessID:4516, Time:6/27/2016 3:16:09 PM, Message]
OnDevicePresenceCheckEvent() fired
```

When HP WS Pro Proxy Agent detects a new printer, HPWSProxyService is restarted and the following log messages are in the log file:

```
DetectedDeviceCount = 1 HostedDeviceCount = 0Detected mismatch in
detected device count and Proxy hosted device count. Restarting
proxy...
```

- LogDetectedPrinterInfo (HP WS Pro Proxy Agent 10.4.1 and later)

If the value of LogDetectedPrinterInfo is changed to true, the value of LogLevel must be changed to All. After the changes are made and HPWSProxyService is restarted, the information about the USB-connected printer that is received from Windows is logged in the DeviceManager.log file.

The following is an example of the log data:

```
[ProcessID:5136, Time:6/27/2016 5:54:11 PM, Message] USB Printer
Name : HP LaserJet Pro M402-M403 n-dne PCL.6[ProcessID:5136,
Time:6/27/2016 5:54:11 PM, Message] USB Printer Port :
USB002[ProcessID:5136, Time:6/27/2016 5:54:11 PM, Message] USB
Printer Driver Name : HP LaserJet Pro M402-M403 n-dne
PCL.6[ProcessID:5136, Time:6/27/2016 5:54:11 PM, Message] USB
Printer Printer Status : Ready
```

- LogLedmAdapterClientIPLogging (HP WS Pro Proxy Agent 10.4.1 and later)

After the value of LogLedmAdapterClientIPLogging is changed to true and HPWSProxyService is restarted, the HPWSProxyLog.log file shows the IP address of the requestor, which is normally HP Web Jetadmin. LogLedmAdapterClientIPLogging is set to the off state by default because IP address resolution *might* cause a delay on an LEDM adapter that receives a lot of requests.

Due to the nature of various network set ups, the IP address might not reflect the true IP address of the source. For example, the address in the log might not be the actual address of the HP Web Jetadmin host.

The following is an example of a message:

```
[ProcessID:5136, Time:6/27/2016 4:58:16 PM, All] Received request
from the (may not be accurate) IP : 10.20.18.196
```

UIO test tool

HPWSProxyService uses Universal I/O DLLs (UIO DLLs) to communicate with PC-connected devices over USB. You can use the UIO test tool to determine if a problem is caused by the UIO DLLs, device, or other proxy components.

Use the following steps to execute the UIO test tool:

1. Double-click the UIOTest.exe file. This file is located in the HPWSProxy\bin\ directory.
2. From the **Select Printer** list, select the USB-connected printer. This list includes the printers that were previously connected, but are now disconnected. This list is the same as the list shown in **Control Panel > Hardware and Sound > Devices and Printers**.
3. Select a printer type: **FuturesSmart**, or **LEDM** for non-FutureSmart devices. For FutureSmart devices, skip to step 6. For LEDM devices, continue to step 4.
4. From the **Select LEDM Tree** list, select a tree element.
5. Click the **Get On All the Trees** or **Get On A Selected Tree** button.
6. Select a Service Urn from the drop down menu.

Note HP WS Pro Proxy Agent 10.3.8 and earlier, these files are located in one of the following directories:

7. Click **Get**.

The results are written in the UIOLog.txt file. This file is in the same directory as the UIOTest.exe file. Prior to HP WS Pro Proxy Agent 10.3.8, this file was created in the C:\temp directory. For HP WS Pro Proxy Agent 10.4.1 and later, the results are also written in the display pane.

The following are examples of log entries:

```
Time:24/06/2016 11:11:08, The tree is:
/DevMgmt/MediaHandlingDyn.xml And The Response is null
Time:24/06/2016 11:09:26, The tree is:
/DevMgmt/DiscoveryTree.xml And The Response Status Code is : 200
Time:24/06/2016 11:09:33, The tree is: /TestNode/ExpectFailure
And The Response Status Code is : 404
```

Response Status Code null means: printer is connected
Response Status Code 200 means: printer is responding correctly
Response Status Code 404 means: endpoint not existing (while printer is connected)
Other Response Status Code might be different per device model.

HP SNMP Proxy Agent logging

The Dbgview.exe program, which is available from technet.microsoft.com/en-us/sysinternals/bb896647, can be used to gather clues on the machine where HP SNMP Proxy Agent is installed that might help determine why discoveries for directly connected devices are not occurring.

1. Use a text editor to create a file named EnableProxyLogging.reg that has the following text:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\HP SNMP Proxy]
"PMLInterface"=dword:00000001
"HP_PROXY_AGENT"=dword:00000001
"PML_INFO_HANDLER"=dword:00000001
"PJL_INFO_HANDLER"=dword:00000001
"PJLInterface"=dword:00000001
```

2. Double-click the EnableProxyLogging.reg script. Regedit launches.
3. Start Dbgview.exe.
4. Restart the SNMP service.

When the SNMP service restarts, you should see debugging messages in Dbgview.exe.

HP WS Pro Proxy logging

To enable full logging in HP WS Pro Proxy Agent, use the following steps on the machine where the LEDM device is directly connected:

1. Open the ProxyServiceConfig.txt file in a text editor. This file is available in the following directory:

C:\Program Files (x86)\Hewlett-Packard Company\HPWSProxy\HPWSProxy\bin

2. The default log level is <Error>. Change the log level to <All>.
3. Use a text editor to create a file named UIOLoggingOn.reg that has the following text:

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\HP\NG\Logging]
"LogInfoDetailLevel"=dword:00000007
"LogCategories"=dword:3e00fff7
"LogOptions"=dword:0e000000
"LogFileName"="C:\uio.log"
"LogParmsPollTime"=dword:0000001e

[HKEY_USERS\S-1-5-18\Software\HP\NG\Logging]
"LogInfoDetailLevel"=dword:00000007
"LogCategories"=dword:3e00fff7
"LogOptions"=dword:0e000000
"LogFileName"="C:\uio.log"
"LogParmsPollTime"=dword:0000001e
```

4. Execute the UIOLoggingOn.reg file.

WMI

If the HP SNMP Proxy Agent discovery attempts fail, HP Web Jetadmin attempts to communicate with a workstation via WMI to extract the plug-and-play registry entry for any physically connected device as long as valid credentials are supplied. The following steps might help to troubleshoot cases where HP Web Jetadmin does not find directly connected devices and the discovery log does not provide enough useful information:

1. WMI must be enabled on each workstation where a device is connected.
2. Administrator rights on the client machines are required to successfully run the WMI commands.
3. Printers must be plug-and-play to be discovered. If Windows believes a device is physically connected, the following registry entries might exist, depending on the port in use:
 - HKLM\System\CurrentControlSet\Enum\LPTENUM
 - HKLM\System\CurrentControlSet\Enum\USBPRINT
 - HKLM\System\CurrentControlSet\Enum\DOT4
 - HKLM\System\CurrentControlSet\Enum\DOT4PRT
 - HKLM\System\CurrentControlSet\Enum\DOT4USB

Each of these folders contain additional folders representing devices that Windows believes might be connected to the designated port. A folder named Control exists in those device folders that Windows believes are physically connected at that particular time.

The USBPRINT folders are dynamic. The Control folder exists when the device is connected and does not exist when the device is disconnected.

The LPTENUM folders are not dynamic. The Control folder exists when the device is connected via LPT1 only after a workstation reboot is performed. The same holds true when a device is disconnected from LPT1. The Control folder is not removed until the workstation is rebooted. Therefore, it is possible that a PC-connected device discovery might report that a device is connected to LPT1 when in fact the device is physically disconnected.

4. Use the Microsoft wbemtest.exe file to determine whether the workstation successfully represents the directly connected device in the registry by simulating the same WMI calls that HP Web Jetadmin makes. Launch wbemtest.exe, and connect to a remote machine by entering the machine name as part of a URL, such as \\machine_name\root\cimv2 (Figure 8). Click **Query** (Figure 9) to run the select *from win32_pnpendentity command and simulate a WMI call to see what plug-and-play devices are found on the workstation. If plug-and-play devices are recognized as connected, entries exist under the ports, such as USBPRINT, DOT4PRT, and LPTENUM (Figures 10 and 11).

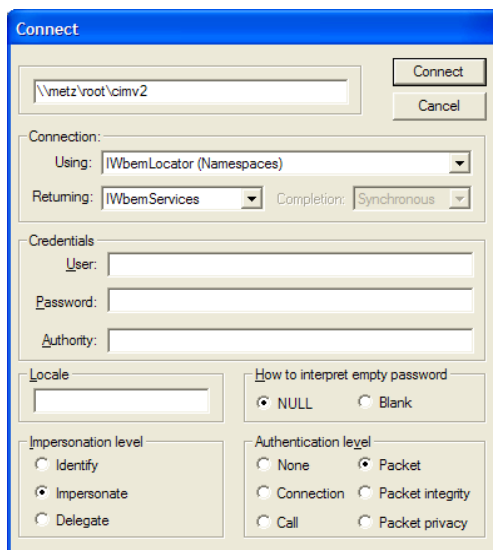


Figure 8

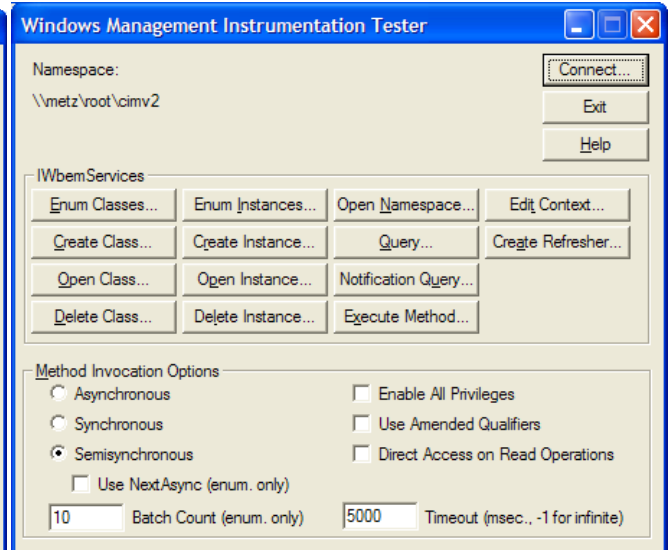


Figure 9

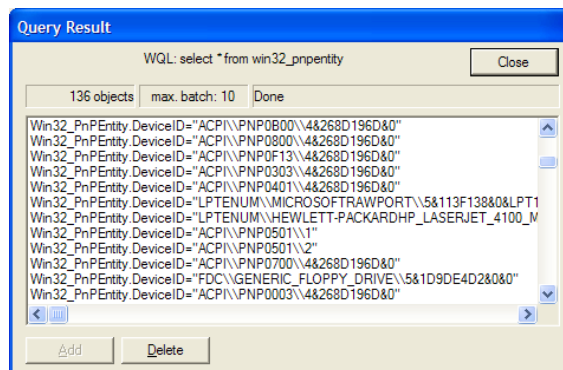


Figure 10

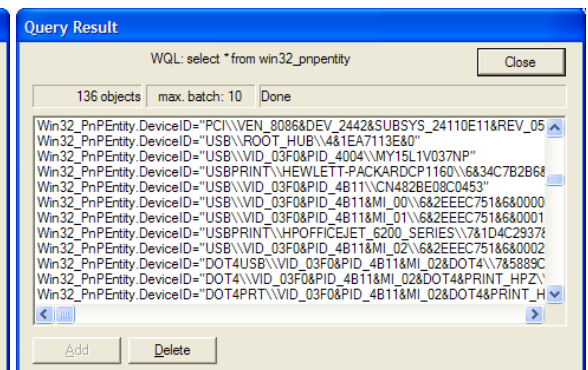


Figure 11

5. If the Windows Firewall is enabled, the workstation might have to be configured to allow HP Web Jetadmin to make WMI calls to successfully discover devices. The Windows Firewall

blocks many ports and services, including remote administration. The procedure for enabling remote WMI calls is outlined in a Microsoft Developer Network (MSDN) technical note titled *Connecting through Windows Firewall*. Run the following command at a remote client to allow remote administration using WMI:

```
netsh firewall set service RemoteAdmin enable
```

Windows XP SP2 includes a built-in firewall that is enabled by default to minimize the chance of attacks on a machine. This firewall can cause access-denied errors when the remote computer and the accounts used for remote connections are not properly configured. When obtaining data from a remote machine, WMI must establish a Distributed Component Object Model (DCOM) connection from local computer to remote computer. To establish this connection, both Windows Firewall and DCOM on the remote computer must be configured correctly to avoid access-denied errors. The configuration must be done locally on the remote machine by changing **Group Policy** settings, executing NETSH commands, or executing a script.

PERFORMANCE

WMI interrogations can be intensive on some workstations. If WMI discoveries take too long to complete, use the following steps to help speed up the discoveries:

1. Enabling WMI on the client's firewall is not sufficient for good performance. While the WMI resolver eventually resolves the device, Windows spends large amounts of time trying to find an enabled communication protocol. Disable the client's firewall altogether to greatly improve WMI performance.
2. After the authorized administrative user's profile is loaded into the PC client, the WMI resolver can obtain device information from the remote PC fairly quickly after it attempts to determine if HP SNMP Proxy Agent is installed. If it is known that HP SNMP Proxy Agent is not installed on any workstation, which prevents HP Web Jetadmin from attempting to discover devices, the WMI resolver can save several seconds per workstation. To skip the HP SNMP Proxy Agent resolver step during discoveries, open a text editor and paste the following text into the file:

```
<ipmc:configuration xmlns:ipmc="www.hp.com/schemas/imaging/ipmc/config/2004/02/24">  
  <property name="SkipProxy">  
    <type>HP.Imaging.Wjp.Sdk.Core.Framework.ConfigurationItemString</type>  
    <value>yes</value>  
  </property>  
</ipmc:configuration>
```

3. Save the file and place it in the following directory:
C:\Documents and Settings\NetworkService\Local Settings\Application Data\HP Inc\HPWebJetadmin\WjaService\config\ResolverMethodPC.config.xml
4. Restart the HP Web Jetadmin service (HPWJA Service).

SUMMARY

HP Web Jetadmin provides two separate techniques for remotely discovering PC-connected devices. These techniques eliminate the need for physical inventories and provide administrators with the flexibility to choose an appropriate tactic. Each technique has advantages and disadvantages. However, proxy agents are generally the preferred method because they provide better management capabilities for PC-connected devices.

APPENDIX A—SUPPORTED PRINTING DEVICES

HP SNMP Proxy Agent, supported legacy devices

The following table lists the printing devices that potentially can be successfully discovered via HP SNMP Proxy Agent using either the discreet DOT4-capable driver typically contained in the printing system bundle included with the device or the HP Universal Print Driver (UPD). HP highly recommends HP UPD because it does not involve searching the Web for a supported DOT4 driver. See the HP UPD websites for a list of the UPD support devices.

HP Color LaserJet 2550 series	HP Deskjet F4180	HP LaserJet M5035 MFP	HP Photosmart 7700 series
HP Color LaserJet 2605	HP Deskjet F4400	HP LaserJet MFP M426	HP Photosmart 7800 series
HP Color LaserJet 2700	HP LaserJet 1010	HP LaserJet M9040/50 MFP	HP Photosmart 7900 series
HP Color LaserJet 2700n	HP LaserJet 1012	HP LaserJet P2015	HP Photosmart 8000 series
HP Color LaserJet 2820 series	HP LaserJet 1015	HP LaserJet P2015d	HP Photosmart 8200 series
HP Color LaserJet 2830 series	HP LaserJet 1150	HP LaserJet P2055/P2035	HP Photosmart 8700
HP Color LaserJet 2840 series	HP LaserJet 1160 series	HP LaserJet P3004 series	HP Photosmart A310
HP Color LaserJet 3000	HP LaserJet 1300	HP LaserJet P3005 series	HP Photosmart A430 series
HP Color LaserJet 3500	HP LaserJet 1300n	HP LaserJet P4014/15	HP Photosmart A510 series
HP Color LaserJet 3550	HP LaserJet 1312 MFP	HP Officejet 4100	HP Photosmart A610 series
HP Color LaserJet 3600	HP LaserJet 1320 series	HP Officejet 4105	HP Photosmart A710 series
HP Color LaserJet 3700	HP LaserJet 2200	HP Officejet 4200 series	HP Photosmart C3100 series
HP Color LaserJet 3800	HP LaserJet 2300	HP Officejet 4300 series	HP Photosmart C4100 series
HP Color LaserJet 4600	HP LaserJet 2300L	HP Officejet 5500 series	HP Photosmart C4200
HP Color LaserJet 4610	HP LaserJet 2410	HP Officejet 5600 series	HP Photosmart C4500 series
HP Color LaserJet 4650	HP LaserJet 2420	HP Officejet 5700	HP Photosmart C5100 series
HP Color LaserJet 4700	HP LaserJet 2430	HP Officejet 6100	HP Photosmart C6100 series
HP Color LaserJet 4730 MFP	HP LaserJet 3015	HP Officejet 6200 series	HP Photosmart C6300 series
HP Color LaserJet 5550	HP LaserJet 3020	HP Officejet 6300 series	HP Photosmart C7100 series
HP Color LaserJet 9500 MFP	HP LaserJet 3027	HP Officejet 7200 series	HP Photosmart D5060
HP Color LaserJet CM1512nfi	HP LaserJet 3030	HP Officejet 7300 series	HP Photosmart D5100 series
HP Color LaserJet CM1312	HP LaserJet 3050	HP Officejet 7400 series	HP Photosmart D6100 series
HP Color LaserJet CM2320	HP LaserJet 3052	HP Officejet 7580	HP Photosmart D7100 series
HP Color LaserJet CM 6040 MFP	HP LaserJet 3055	HP Officejet 7680/7780	HP Photosmart D7200 series
HP Color LaserJet CP1505	HP LaserJet 3380	HP Officejet 9100 series	HP Photosmart D7300 series
HP Color LaserJet CP1515/18	HP LaserJet 3390	HP Officejet J2100 series	HP Photosmart Pro B9100 series
HP Color LaserJet CP202x	HP LaserJet 3500	HP Officejet Pro K5300	HP PSC 1000
HP Color LaserJet CP2025	HP LaserJet 4200	HP Officejet Pro K5400 series	HP PSC 1100
HP Color LaserJet CP3505	HP LaserJet 4240	HP Officejet Pro K5600	HP PSC 1200
HP Color LaserJet CP3515	HP LaserJet 4250	HP Officejet Pro K8600	HP PSC 1300 series
HP Color LaserJet CP3525	HP LaserJet 4300	HP Officejet Pro L7300	HP PSC 1310 series
HP Color LaserJet CP4005	HP LaserJet 4350	HP Officejet Pro L7500	HP PSC 1358
HP Color LaserJet CP6005	HP LaserJet 5200	HP Officejet Pro L7600	HP PSC 1400 series
HP Color LaserJet CP6015	HP LaserJet 5200lx	HP Officejet Pro L7700	HP PSC 1500 series
HP Color LaserJet CP9505	HP LaserJet 8150	HP Photosmart 140 series	HP PSC 1600 series
HP Color LaserJet M452	HP LaserJet 9000	HP Photosmart 240 series	HP PSC 2100
HP Color LaserJet MFP M477	HP LaserJet 9040 MFP	HP Photosmart 2570 series	HP PSC 2150
HP Color LaserJet Pro M252	HP LaserJet 9050	HP Photosmart 2600 series	HP PSC 2170
HP Deskjet 450	HP LaserJet 9050mfp	HP Photosmart 2700 series	HP PSC 2200
HP Deskjet 5400 series	HP LaserJet 9500	HP Photosmart 3100 series	HP PSC 2300 series
HP Deskjet 5900 series	HP LaserJet CM1410 Series	HP Photosmart 3200 series	HP PSC 2350 series
HP Deskjet 6600 series	HP LaserJet CP1520 Series	HP Photosmart 330 series	HP PSC 2400 series
HP Deskjet 6800 series	HP LaserJet M1522nf	HP Photosmart 3300 series	HP PSC 2500 series
HP Deskjet 6980	HP LaserJet M1530 Series	HP Photosmart 380 series	HP Scanjet 7000 s2
HP Deskjet 9800	HP LaserJet M2727 MFP	HP Photosmart 420 series	HP Scanjet 7500
HP Deskjet D1600	HP LaserJet M3027 MFP	HP Photosmart 440	HP Scanjet Enterprise Flow 5000
HP Deskjet D2600	HP LaserJet M3035 MFP	HP Photosmart 470 series	HP Scanjet 9000
HP Deskjet F300 series	HP LaserJet M4345 MFP	HP Photosmart 7200 series	HP Scanjet N9120
HP Deskjet F4100	HP LaserJet M5025	HP Photosmart 7600 series	

HP SNMP Proxy Agent, not supported: HP FutureSmart devices

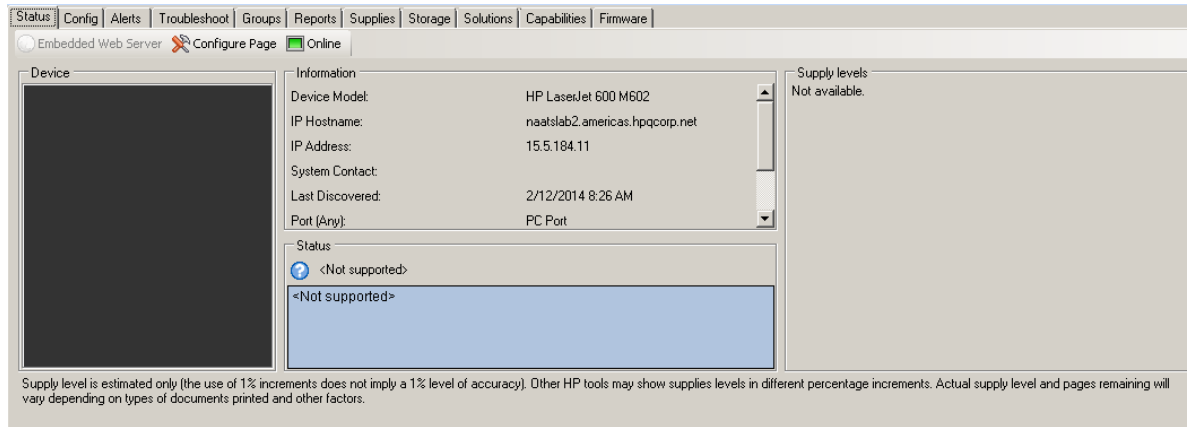
HP SNMP Proxy Agent can discover the following devices, but only the model name is displayed, nothing more. HP Web Jetadmin uses Web Services to manage these devices. SNMP Proxy Agent does not pass Web Services. This means that initially the total page count might be displayed during device discovery because HP Web Jetadmin only uses SNMP during discoveries. However, after HP Web Jetadmin identifies the device model, it uses the adequate communication protocol (Web Services for HP FutureSmart devices) and items such as total page count are no longer displayed.

Therefore, HP Web Jetadmin does not support PC-connected HP FutureSmart devices.

The following are examples of HP FutureSmart devices:

- HP Color LaserJet CM 4540 MFP
- HP Color LaserJet CP5520
- HP Color LaserJet Enterprise M750
- HP Color LaserJet Enterprise M855
- HP Color LaserJet Enterprise flow MFP M880
- HP LaserJet 500 MFP M525
- HP LaserJet Enterprise 500 MFP MXP M525
- HP LaserJet 500 color M551
- HP LaserJet 500 color MFP M575
- HP LaserJet Enterprise 500 Color MXP M575
- HP LaserJet 600 M601
- HP LaserJet 600 M602
- HP LaserJet 600 M603
- HP LaserJet 700 MFP M725
- HP LaserJet 800 M806
- HP LaserJet flow MFP M830
- HP LaserJet M4555 MFP
- HP Color LaserJet Flow M680
- HP Color LaserJet M680
- HP Color LaserJet M651
- HP Officejet Color flow MFP X585
- HP Officejet Color MFP X585
- HP Officejet Color X555
- HP LaserJet Enterprise MFP M630

In the following example of a USB-connected HP LaserJet M602 device, notice that only the model name is displayed. HP Web Jetadmin uses Web Services to extract and display everything else, including the device image.



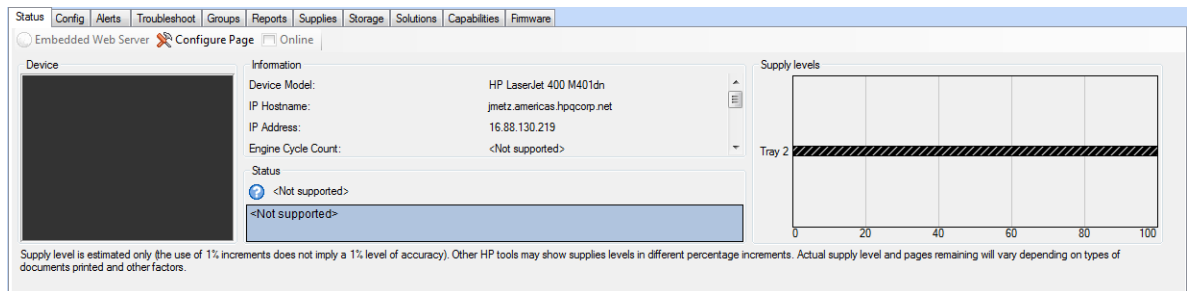
HP WS Pro Proxy Agent, supported devices

HP WS Pro Proxy Agent can discover the following devices. HP SNMP Proxy Agent might also discover some of these devices. However, HP recommends that you use HP WS Pro Proxy Agent to discover these devices so that the most features are supported because HP Web Jetadmin used LEDM to extract and display most features.

- HP Color LaserJet Pro M252
- HP Color LaserJet Pro M452
- HP Color LaserJet Pro MFP M274n
- HP Color LaserJet Pro MFP M277n
- HP Color LaserJet Pro MFP M476
- HP Color LaserJet Pro MFP M477
- HP Officejet Pro 8000 Enterprise
- HP Officejet Pro 8500A
- HP Officejet Pro 8100 Series
- HP Officejet Pro 8210
- HP Officejet Pro 8600 Series
- HP Officejet Pro 8610/8620/8630
- HP Officejet Pro 8710/8720/8730
- HP Officejet Pro X451/X551
- HP Officejet Pro X476/X576
- HP Officejet Pro 251
- HP Officejet Pro 276
- HP LaserJet CM1415
- HP LaserJet CP1525
- HP LaserJet M1536
- HP LaserJet Pro 200 color M251
- HP LaserJet Pro 200 color M276
- HP LaserJet Pro 300 color M351
- HP LaserJet Pro 300 color MFP M375
- HP LaserJet Pro 400 color M451
- HP LaserJet Pro 400 color MFP M475
- HP LaserJet Pro 400 Printer M401
- HP LaserJet Pro 400 MFP M425
- HP LaserJet Pro 500 color MFP M570
- HP LaserJet Pro M201

HP LaserJet Pro M202
HP LaserJet Pro M402
HP LaserJet Pro M501
HP LaserJet Pro M701/706
HP LaserJet Pro MFP M225
HP LaserJet Pro MFP M226
HP LaserJet Pro MFP M427
HP LaserJet Pro MFP M435
HP LaserJet Pro MFP M521
HP PageWide Pro 452dw
HP PageWide Pro 552dw
HP PageWide Pro MFP 477dw
HP PageWide Pro MFP 577dw

The following is an example of an HP LaserJet M401 device that was discovered via HP SNMP Proxy Agent. Notice that only the model name and tray gauges are displayed because HP Web Jetadmin uses LEDM to obtain everything else. HP WS Pro Proxy Agent displays a much fuller set of features for the HP LaserJet M401 because it can understand the LEDM queries that HP Web Jetadmin uses.



Note Tray gauges are actually obtained using SNMP and not LEDM, so they are missing when the device is discovered via HP WS Pro Proxy Agent.

APPENDIX B—HP WEB JETADMIN SUPPORT FOR TELECOMMUTER DEVICES

Millions of people around the world now work from home offices, remote work areas, and other places outside of traditional office environments. By allowing employees to telecommute, organizations can reduce real estate requirements, improve worker productivity, conserve energy, and facilitate emergency readiness plans. Employees cut their commuting costs and gain greater flexibility in their work schedules. This flexibility is particularly important when employees are part of a global team that meets outside of typical office hours.

To support the needs of the remote workers, HP offers a broad portfolio of imaging and printing products, solutions, and services designed with telecommuters in mind. In fact, you can use HP Web Jetadmin to continue managing and monitoring the printers of employees who work from home.

HP Web Jetadmin provides the following capabilities for those telecommuter printing devices:

- IT can monitor telecommuter devices by noting their presence and identifying them within the network.
- IT can view and configure telecommuter devices for easier remote troubleshooting and can subscribe to supplies alerts.
- IT can keep track of telecommuter devices and supply usage to better manage costs and environmental impact.
- IT can receive world-class assistance through HP Web Jetadmin Premium Support.

HP Web Jetadmin best practices for managing telecommuter devices

HP recommends that IT use the following best practices for the most effective management of the remote printing devices that telecommuters use:

- Install HP SNMP Proxy Agent and a supported driver on telecommuter PCs and laptops. For more information, see “Proxy agents” on page 3. If WMI discovers the printer, the printer model is the only information that is displayed on the **Status** page and device configuration is not available.
- Determine the organization’s telecommuter discovery and collection policies. HP recommends setting a standard IP address range for telecommuter VPN access. These are the IP addresses distributed to telecommuter workstations as they log on to the network through VPN. These ranges might have to be obtained from the IT team responsible for the VPN infrastructure. Since IP addresses might change regularly, limiting the IP address range makes new discoveries faster and more successful.
- Because IP addresses often change, schedule a more frequent discovery based on the IP address range. The best time for discovery depends on the following factors:
 - The size of the telecommuter IP address range.
 - When you expect telecommuters to be connected. You can run several discoveries at different times for different global locations.
- Create an auto group for the telecommuter devices in that IP range and set the following policies for this auto group:
 - Set device-specific features
 - Schedule a more frequent data collection that includes device usage, supplies, and inventory
 - Subscribe to supply alerts

- Export data daily to email, a database, or other reporting tools—including page counts, supply level data, and more

All of the PC-connected troubleshooting tips outlined in this white paper also apply to telecommuter devices if the PC is connected via VPN and the device is connected via USB.

© Copyright 2017 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

VMware® is a registered trademark of VMware, Inc.

c01840676EN, Rev. 19, April 2017

